Software Assurance CBK/Principles Organization

The Department of Homeland Security (DHS) Software Assurance Program is seeking review and comment on Software Assurance: A Curriculum Guide to the Common Body of Knowledge to Produce, Acquire, and Sustain Secure Software and the associated SwA CBK-Principles Matrix. The CBK-Principles-SANS SSI Matrix and Principles Organization: Towards an Organization for Software System Security Principles and Guidelines (version .26a) are also available for reference and review.

The comment period on version 1.2 of the Curriculum Guide is closed. However, comments are still welcome, but they may not be reflected in the next release. Please use the comment form[1] and submit comments to Samuel Redwine[2].

Software Assurance: A Curriculum Guide to the Common Body of Knowledge to Produce, Acquire, and Sustain Secure Software[3] (referenced in short as SwA CBK) provides a framework intended to identify workforce needs for competencies, leverage sound practices, and guide curriculum development for education and training relevant to software assurance. Because software quality assurance (SQA) and software engineering have evolved bodies of knowledge that do not explicitly address security as a quality attribute, and the National Strategy to Secure Cyberspace[4] Action/Recommendation 2-14 relating to software assurance (SwA) focused on security, integrity and reliability, the initial focus of SwA education has been to "complete" relevant academic programs. The initial focus for SwA therefore has been for persons with knowledge of SQA and software engineering but not security.

SwA CBK-Principles Matrix[5]
CBK-Principles-SANS SSI Matrix[6]

Towards an Organization for Software System Security Principles and Guidelines[7] Version 1.0 contains an extensive set of software system security principles and guidelines organized in a logical, in-depth fashion. As well as providing coherence, the structure provides grounds for arguing completeness - at least at the higher levels. Historically, principles and guidelines for software system security have originated variously over thirty-plus years, and their authors have tended to provide flat lists occasionally organized topically, by major life-cycle stages, or by the author's judgment of importance. The result was hundreds of items whose relationships to each other were unclear and therefore hard to systematically learn, remember, and teach. This document provides previously lacking coherence and completeness.

This is the first highly organized presentation of such a comprehensive set of principles and guidelines. Its structure emphasizes how they relate to each other. The organization aims to start with the most basic, abstract, or inclusive ones and recursively identify the ones that are logically subordinate to each - generally as parts, partial solutions, or causes of them. Thus, it aims to begin to bring needed coherence and intellectual manageability to the area.

1. http://buildsecurityin.us-cert.gov/bsi/926-BSI.html (CBK_Principles_Comments_Sheet_Oct_2007)
2. mailto:redwinst@cs.jmu.edu
3. http://buildsecurityin.us-cert.gov/bsi/940-BSI.html (CurriculumGuideToTheCBK)
4. http://www.whitehouse.gov/pcipb/
5. http://buildsecurityin.us-cert.gov/bsi/923-BSI.html (SwA CBK-Principles Matrix)
6. http://buildsecurityin.us-cert.gov/bsi/924-BSI.html (CBK-Principles-SANS SSI Matrix)
7. http://www.jmu.edu/iiia/webdocs/Reports/SwA_Principles_Organization-sm.pdf